UNITED STATES DISTRICT COURT
DISTRICT OF DELAWARE

IN RE GOOGLE INC. COOKIE PLACEMENT CONSUMER PRIVACY LITIGATION	C.A. 12-MD-2358 (SLR)
This Document Relates to: **All Actions**	

DEFENDANT GOOGLE INC.'S
OPENING BRIEF IN SUPPORT OF ITS
MOTION TO DISMISS THE CONSOLIDATED AMENDED COMPLAINT

MICHAEL H. RUBIN, CA Bar No. 214636
ANTHONY J WEIBELL, CA Bar No. 238850
C. SCOTT ANDREWS, CA Bar No. 243690
WILSON SONSINI GOODRICH & ROSATI
Professional Corporation
650 Page Mill Road
Palo Alto, CA 94304-1050
Telephone: (650) 493-9300
Facsimile: (650) 565-5100
E-mail: mrubin@wsgr.com; aweibell@wsgr.com;
sandrews@wsgr.com

Attorneys for Defendant
GOOGLE INC.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

CONSTITUTIONS AND STATUTES

RULES

STATEMENT OF THE PROCEEDINGS

Whenever a story about a snafu at a popular technology company appears in the press, lawsuits are filed *en masse*. These lawsuits invariably seek windfall recoveries under esoteric and inapplicable statutes regardless of whether anyone suffered any actual injury. And virtually without exception, courts have dismissed such cases at the pleading stage either for lack of standing or for failure to state a claim. This action should be no exception.

This multidistrict litigation ("MDL") consists of 24 consolidated civil actions brought on behalf of putative nationwide classes of individuals who allegedly used the Apple Safari and/or Internet Explorer web browsers to visit websites on which Google Inc. ("Google") and other defendants displayed advertisements. Four named plaintiffs ("Plaintiffs") filed a consolidated amended complaint ("CAC") against Google, PointRoll, Inc., Vibrant Media, Inc., Media Innovation Group LLC, and WPP, plc (collectively "Defendants"). With respect to Google, Plaintiffs allege that when it showed them advertisements, Google placed "cookies" on their browsers even though their browsers' settings suggested that such cookies would be blocked. Plaintiffs further allege that by placing these cookies, Google was able to recognize the browser each time it visited a site displaying a Google ad, allowing Google to tailor ads based on the sites the browser previously visited.

Plaintiffs have not been harmed by the conduct about which they complain. Accordingly, they lack standing. Regardless, Plaintiffs have failed to state a claim under either the statutory or common law theories they advance. For both reasons, this action should be dismissed.

SUMMARY OF THE ARGUMENT

1. Plaintiffs lack Article III standing**.** Google's alleged placement of cookies on Plaintiffs' browsers did not cause them any cognizable injury. To the extent that the presence of Google's cookies affected Plaintiffs at all, it was only in that they might have seen different Google ads than the ones they otherwise would have seen. The only thing Google obtained by

virtue of the cookies' presence was the "cookie value"—a string of characters that Google generates to identify an individual browser (*e.g.*, id="225f401f5201002e||t=1328801360|et=730|cs=002213fd4890910dc3faab6200). Although Plaintiffs suggest that the cookies Google places on browsers enable Google to collect personal information, these cookies collect nothing, have nothing whatsoever to do with the content of any of the communications between Plaintiffs' browsers and Google, and in no way constitute, contain or reveal "personal information." Plaintiffs' allegations—that they "gave up more personal information in their dealings with Google than they would have," "received less privacy from Google than promised them," and "lost the opportunity to sell the personal information at full value"—are the sort of lawyer-concocted conclusions that courts routinely have ruled insufficient to establish Article III standing. They are also refuted by the materials Plaintiffs incorporate by reference in the CAC, which show that Google received no personal information from the alleged placement of the cookies at issue.

2. Each of Plaintiffs' claims fails as a matter of law because Plaintiffs do not allege basic elements of the claim:

- The Wiretap Act claim and related state law claim (Counts I and VIII) fail (i) because Google was a party to the communications between it and Plaintiffs' browsers, or because Google had the prior consent of a party to the communication to receive them, and (ii) the placement and presence of cookies about which Plaintiffs complain did not enable Google to obtain any information about the substance, purport or meaning of their communications.

- The Stored Communications Act claim (Count II) fails because (i) Plaintiffs themselves allege that the communications between their browsers and Google were obtained while *in transit*, not in "storage," (ii) Plaintiffs' computers and phones are not "facilities" under the SCA, and (iii) Plaintiffs cannot show that Google lacked authorization to access their browsers' communications with Google.

- The Computer Fraud and Abuse Act claim and related state computer fraud claim (Counts III and VII) fail because Plaintiffs can neither allege that (i) any "damage" or "loss" (ii) nor any unlawful "hacking" occurred.
- The invasion of privacy and intrusion upon seclusion claims (Counts IV and V) fail because Plaintiffs cannot allege an (i) intrusion into a private matter (ii) that was "highly offensive to a reasonable person."
- The California Consumer Legal Remedies Act claim (Count IX) fails because Plaintiffs cannot allege any (i) "damage" (ii) in connection with the "purchase or lease" (iii) of a "good or service," or (iv) that they provided the 30-day pre-filing notice required by the Act.
- The California unfair competition claim (Count VI) fails because Plaintiffs did not (i) personally (ii) lose any money or property (iii) due to the alleged conduct.

STATEMENT OF FACTS

A. Factual Background

1. Cookies and Browsers

Computer "cookies" are commonplace in Internet advertising, and regularly used to store website preferences, retain the contents of shopping carts between visits, and keep browsers logged into social networking services and webmail as they surf the Internet. Technically, cookies are small text files containing pieces or "strings" of text that websites and services such as advertisers transmit to browsers, including Internet Explorer, Safari, and Google Chrome. CAC ¶¶ 38-39; *In re Pharmatrak, Inc.*, 329 F.3d 9, 23 (1st Cir. 2003). Although a service may send a cookie to a browser, whether or not the browser accepts the cookie depends on the browser and its settings. If the design and setting of the browser allow it to accept the cookie, the cookie will be placed on the browser. *Pharmatrak*, 329 F.3d at 14; *see generally In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001) (describing cookie function).

Cookies are useful for Internet advertising because they allow more relevant ads to be displayed. While browsing the Internet, browsers automatically submit certain information to

the websites and services they connect to (*e.g.*, the type of browser, the operating system of the computer, the address of the website the browser is displaying, the IP address from which the computer is connected to the Internet, and the computer's screen resolution ("Browser-Generated Information")). CAC ¶¶ 31, 46. Browsers submit this information so that the web sites and services to which they are connecting can display the correct content.[1] If a browser has a cookie from a given site or service on it, when it connects to that site or service, the browser will transmit the cookie value along with the Browser-Generated Information. This is useful for the website or service because it is in that manner that the Browser-Generated Information can be correlated and associated with an individual browser and used to tailor the content shown to that browser. *Id.* ¶ 46.

2. Google and the DoubleClick ID Cookie

Google "is a global technology leader focused on improving the ways people connect with information." CAC ¶ 19. In addition to its renowned search and email services, Google operates an advertising network that can display "tailored" ads in browsers. *See id.* ¶ 43. Google uses a cookie called the DoubleClick ID Cookie to enable tailored ads.

Assuming a browser's design and setting allow it to accept cookies, the DoubleClick ID Cookie will be placed on a browser during the normal exchange of information that accompanies the display of a Google ad in a browser. *See, e.g., id.* ¶ 45. Once on a browser, the DoubleClick ID Cookie allows Google to recognize when browsers visit websites displaying ads from the Google advertising network and to correlate the Browser-Generated Information for individual browsers. *See generally DoubleClick*, 154 F. Supp. 2d 497 (describing how DoubleClick ID Cookie functions). Google uses aggregated Browser-Generated Information from a given browser to tailor ads that may be more relevant to a user of that browser than the ads that would be shown if the browser did not have a cookie on it. *Id.*

[1] It is during that exchange of information—Browser-Generated Information flowing to the website and advertising service, and website content and ads flowing back to the browser—that cookies are usually placed on browsers. CAC ¶ 45.

The DoubleClick ID Cookie itself neither contains nor collects any information. It consists only of an anonymous cookie value. The Browser-Generated Information that the DoubleClick ID Cookie correlates is anonymous, and Google maintains its anonymity by keeping it segregated from the account data that resides in Google accounts, such as Gmail. CAC ¶ 102. Users who do not wish to see ads from Google tailored using the DoubleClick ID Cookie can "choose to opt out of the DoubleClick cookie at any time by using DoubleClick's opt-out cookie." RJN Ex. 1 at 3.[2] Browsers with an "opt out" cookie still automatically submit the same Browser-Generated Information to Google, but the "opt out" cookie will signal Google not to correlate or use the information for tailored ads.

3. Google's Development and Use of the Intermediary Cookie

In 2011, Google developed a feature to enable ads that, with users' consent, were tailored to the social connections of users of its Google+ social networking service. This feature, launched in October 2011, enabled logged-in Google+ users to highlight Google ads that they liked. *See* CAC ¶ 101; RJN Ex. 2. Google's goal was to implement this personalization in a privacy and security sensitive manner. Key to Google's design was the development of a new cookie (the "Intermediary Cookie") that allowed its distinct account and advertising systems to interact without commingling personal and anonymous data. *See* CAC ¶¶ 84-94, 101-102. The Intermediary Cookie served as an encrypted and temporary intermediary between a user's Google account (which may contain personal information) and the Google advertising network (which uses anonymous Browser-Generated Information). The purpose of the Intermediary Cookie is to identify if a browser is signed into a Google account, but to do so in a way that does not compromise the anonymity of the advertising data. *See id.* ¶¶ 89, 112. The Intermediary Cookie collects no personal information, is not used to correlate Browser-Generated In-

[2] Citations to "RJN" refer to "Google Inc.'s Request for Judicial Notice and for Consideration of Documents Referenced and Relied Upon in the Consolidated Amended Complaint" submitted herewith.

formation, and is placed from the doubleclick.net domain (the same domain from which the DoubleClick ID Cookie is set). *See id.* ¶¶ 78, 90-95.

4. The Safari Web Browser and How it Handles Cookies

The Safari browser, in its default state, is set to block so called "third party" cookies and often does.[3] CAC ¶¶ 102-103. However, blocking all third party cookies can break certain popular web functions, such as social "like" buttons used to integrate third-party social features into websites. In light of this, instead of blocking all third party cookies, Apple specifically developed and designed for Safari at least three exceptions to its third-party cookie handling policy:

(1) Safari allowed cookies to be placed from a third party domain if, during the process of exchanging information with a third party domain to load third party content, the browser submitted a form to the third party domain (the "Safari Form Submission Rule");

(2) Safari allowed cookies to be placed from a third party domain if one cookie from that domain was already present on the browser (the "Safari One In, All In Rule"); and

(3) Safari allowed all third-party domains to read cookies.

These changes made Safari's cookie-handling policy "less restrictive than many competing browser vendors." RJN Ex. 3.

Safari's Form Submission Rule was known to web programmers, and Facebook recommended the rule as a "best practice" to its developers as a means for delivering a consistent user experience across all browsers. *See* CAC ¶¶ 78, 104-105; RJN Ex. 4. It was the Form Submission Rule that Google used to place the Intermediary Cookie on Safari browsers.[4] Unbeknownst to many, however, Apple had also relaxed Safari's approach to third-party cookies

[3] A "third party" cookie is one placed on a browser by a website or service other than the site the browser is displaying at the time the cookie is set. CAC ¶ 39. A "first party" cookie is a cookie set by the website that is being displayed. *Id.* These terms shed no light on a given cookie's purpose; they merely describe the context in which the cookie is placed on a browser.

[4] As explained above, the Intermediary Cookie does not correlate Browser-Generated Information. It merely identifies if a browser is signed into a Google Account in a way that does not compromise the anonymity of any advertising data associated with the browser.

by adopting another rule, unique among major browsers. Apple designed Safari to accept all cookies from a given domain once a single cookie from that domain was present on the browser (the Safari One In, All In Rule described above). *See id.* ¶¶ 78, 94.

An unforeseen consequence of Safari's One In, All In Rule was that, once an Intermediary Cookie had been placed on a browser, certain Safari browsers would then accept the DoubleClick ID Cookie. That is because both cookies are placed from the same domain (doubleclick.net). *See id.* ¶ 105 (referring to this behavior as "another quirk in Safari"). The Google team that designed the Intermediary Cookie was unaware of Safari's obscure and atypical One In, All In Rule, and did not anticipate or intend that placing an Intermediary Cookie on a Safari browser could also cause the browser to accept a DoubleClick ID Cookie.[5] RJN Ex. 2. To the extent that this unexpected outcome had any effect, it is only that a more tailored ad may have been displayed to the browser than otherwise would have been.[6] And Plaintiffs do not say how they were even affected—they do not allege that the DoubleClick ID Cookie or the Intermediary Cookie (or any other) was ever placed on their own browsers.

5. The Internet Explorer Web Browser and How It Handles Cookies

In its default state, Microsoft's Internet Explorer web browser ("IE") usually allows third party cookies. *See* CAC ¶¶ 179-184. Microsoft designed IE's cookie handling behavior to partially rely on the "P3P" protocol, a voluntary protocol dating from 2002. *Id.* ¶¶ 171-179. P3P purported to allow websites to present their privacy policies to browsers in a machine-readable P3P "Compact Policy Statement" so that browsers could make automatic decisions about how to treat a website's cookies without manual input. *Id.* If a website presents

[5] Had Google intended to place the DoubleClick ID Cookie on Safari browsers in their default state, it could have done so directly using the Safari Form Submission Rule. But the DoubleClick ID Cookie was not placed on browsers using the Form Submission Rule and Plaintiffs do not and cannot allege that it was.

[6] Although the CAC mentions a statement about the behavior of Safari browsers that was posted to a rarely-visited Google Help Center page before the Intermediary Cookie was developed and a year before Apple implemented Safari's One In, All In Rule, CAC ¶ 79, Plaintiffs make no claim to have ever seen or relied upon the statement.

information in a P3P Compact Policy Statement that is not in P3P machine-readable format, the P3P protocol dictates that the information should be ignored and treated as if it "was not present." *Id* ¶ 181.

Plaintiffs allege that IE is supposed to block third party cookies "unless the site includes a P3P Compact Policy Statement, which (1) informs the IE browser how the third-party website will use the cookie, and (2) ensures the IE browser that the third-party cookie will not be used to track the user's Internet activity and communications." *Id.* ¶ 180. According to those allegations, IE should reject third party cookies from a website that presents a Compact Policy Statement lacking the supposedly required information in machine-readable P3P format. But IE does not behave this way. As Plaintiffs recognize, Microsoft actually designed IE to *accept* third party cookies even where a website presents a Compact Policy Statement that both lacks the supposedly required information and includes information written in "human" English that the P3P protocol says should be treated as if it "was not present." *Id.* ¶¶ 183-184.

Presumably, Microsoft does not strictly adhere to the P3P protocol because it is an older protocol that is technically incompatible with many web capabilities, and strict enforcement would discourage users from using IE. *See id.* ¶ 189. Indeed, Facebook, and at least 11,000 other websites do not issue P3P-compliant Compact Policy Statements because of the incompatibility with modern web technology. *Id.* ¶¶ 183, 189; RJN Ex. 5. Because the google.com website is unable to communicate its modern privacy policy in a P3P Compact Policy Statement, each time an IE browser requests such a statement from google.com, the website responds with the plain English message, "This is not a P3P policy!" and directs users to the full version of its privacy policy on its website. CAC ¶ 183. Despite the fact that google.com responds with non-machine-readable language that the P3P protocol dictates should be ignored as "not present," IE is nevertheless designed to accept the response and allow third party cookies on the browser (hereinafter, "the IE Behavior"). *See id.* ¶¶ 183-184.

Like their claims regarding Safari, Plaintiffs' claims about IE are limited to the cookies Google places from the doubleclick.net domain. *Id.* But Plaintiffs' IE-related allegations are

focused on the google.com domain and allege no facts with respect to whether the doubleclick.net domain responds with a P3P Compact Policy Statement before placing cookies on browsers. *See id.* ¶¶ 183-185 & n.107. Nor do Plaintiffs allege that IE would have rejected these cookies if Google's actual privacy policy had been readable by IE in P3P format. In any event, even if a DoubleClick ID Cookie had been placed on Plaintiffs' browsers because of the IE Behavior, the only result is that they may have seen ads more tailored to their interests than ads they would have seen absent the cookie. They would not have been otherwise affected.

6. Placing Cookies on Browsers Did Not Enable Google to Collect Any Personal Information

Plaintiffs allege that Google routinely receives three things when browsers communicate with it:

(1) personal information, such as names and addresses voluntarily given to Google by users that sign up to use the Google+ service and other services on google.com, *see* CAC ¶¶ 97-98, 112-113, 209;

(2) Browser-Generated Information, as described above; and

(3) the random anonymous DoubleClick ID Cookie value that is sent to the doubleclick.net domain each time a browser requests to load a website that displays Google ads, *see id.* ¶¶ 46, 78.

Only the last item—the cookie value—is relevant to Plaintiffs' claims because it is the only thing Google would not receive if a cookie were not present on a browser.[7] Cookies do not *cause* the sending of Browser-Generated Information or any personal information. If any such information is sent to Google, it would happen without regard to a cookie's presence.

Cookies do not enable Google to receive personal information. The personal information Plaintiffs allege Google receives has nothing to do with the cookies at the heart of Plaintiffs' complaint. Google receives the personal information from individuals who affirma-

[7] The value of the Intermediary Cookie is not at issue because, as explained above, this cookie collects no information. It merely represents something Google already knows: whether a browser is currently logged into a Google account. *Id.* ¶¶ 78, 89, 102.

tively sign up to use Google services. *See id.* ¶¶ 97-98, 112-113, 209. Those individuals provide personal information pursuant to Google's terms of use. *See id.*; *see also id.* at 31 n.67. Any allegation that Google received "personal information" is therefore untethered to the conduct Plaintiffs challenge. Personal information would have been received when a user of Google services voluntarily submitted it, not due to Google's use of cookies.

Cookies do not enable Google to receive Browser-Generated Information. Google's receipt of Browser-Generated Information is likewise not attributable to the placement or presence of cookies. Browser-Generated Information is sent to Google each time a browser loads a webpage displaying a Google ad because Browser-Generated Information is needed to properly display an ad. That happens regardless of whether or not that browser has a Google cookie. *See id.* ¶¶ 31-34, 46. And browsers without cookies still see ads on websites. The ads they see are just less tailored and relevant than the ads that would be shown if the browsers had a DoubleClick ID Cookie.

Cookies enable Google's receipt of *cookies*. The only thing Google receives due to the placement and presence of cookies—*i.e.*, the only thing sent to Google that would not be sent if cookies were not present on the browser—is the value of the DoubleClick ID Cookie itself (*e.g.*, id="225f401f5201002e||t=1328801360|et=730|cs=002213fd4890910dc3faab6200). *Id.* ¶¶ 46, 78. That cookie value is neither personal information nor Browser-Generated Information, and is communicated to Google regardless of how it came to reside on a browser.

Plaintiffs *speculate* that these cookies enable Google to comingle the personal information that users provide to Google with the Browser-Generated Information that Google maintains on its separate advertising network. *See id.* ¶ 98. That is nothing more than rank speculation. Plaintiffs do not allege that Google actually comingled and used combined personal information and Browser-Generated Information. In fact, Plaintiffs do not even allege that they are Google account users or that they ever provided *any* personal information to Google that could be comingled.

B. The Complaint and the Named Plaintiffs

Following the publication in February 2012 of news articles describing Safari's Form Submission and One In, All In Rules that allowed the placement of third party cookies on Safari, 24 federal civil actions were filed against Google and other online advertising companies in federal courts across the country. The Judicial Panel for Multidistrict Litigation transferred these actions to this Court for coordination. *See* Dkt. No. 1. All of these actions were later consolidated, and Plaintiffs were directed to file a consolidated complaint. *See* Dkt. No. 22.

On December 19, 2012, Plaintiffs filed the CAC against Defendants. The four named plaintiffs in the CAC are William Gourley, Jose Bermudez, Nicholas Heinrich, and Lynne Krause. Each plaintiff allegedly used the Apple Safari and/or Internet Explorer browsers to visit websites that displayed Google ads. CAC ¶¶ 10-13. Plaintiffs allege that they believed the default settings of their browsers were supposed to block third party cookies like the DoubleClick ID Cookie that allow tailored ads. *Id.* Plaintiffs do not allege that Google modified or changed any settings on their browsers. Plaintiffs instead allege that because of the unique behavior of these browsers described above, Google may have placed cookies on their browsers. *Id.* ¶ 1. In the CAC, Plaintiffs assert various federal and states claims, seeking to represent a putative class of "individuals domiciled in the United States who used the Apple Safari or Microsoft Internet Explorer web browsers and visited a website that deployed third-party tracking cookies from [Defendants]." *Id.*

For the reasons explained below, Plaintiffs' allegations are insufficient to create Article III jurisdiction over this dispute and do not state a cause of action against Google.

ARGUMENT

II. THIS ACTION SHOULD BE DISMISSED UNDER RULE 12(B)(1) BECAUSE PLAINTIFFS LACK ARTICLE III STANDING

The action should be dismissed under Rule 12(b)(1) because Plaintiffs have not suffered an actual injury. Plaintiffs therefore lack standing under Article III of the United States Constitution.

A. Plaintiffs Have No Standing Because They Have Alleged No Actual Injury

A suit brought by a plaintiff without Article III standing does not meet the Constitution's "case or controversy" requirement and should be dismissed for lack of subject matter jurisdiction under Rule 12(b)(1). *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 101, 109-110 (1998). "[T]o satisfy Article III's standing requirements, a plaintiff must show (1) it has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-181 (2000). "In the class action context, that requirement must be satisfied by at least one named plaintiff." *McNair v. Synapse Grp. Inc.*, 672 F.3d 213, 223 (3d Cir. 2012) (citing *Warth v. Seldin*, 422 U.S. 490, 502 (1975) ("Petitioners must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent.")). The plaintiff "bears the burden of establishing that he has Article III standing for each type of relief sought." *ZF Meritor, LLC v. Eaton Corp.*, 696 F.3d 254, 301 (3d Cir. 2012).

Plaintiffs' action should be dismissed for lack of Article III standing because Plaintiffs cannot show any injury from the placement or presence of any Google cookies.[8] As a preliminary matter, Plaintiffs do not allege that they themselves suffered any injury: the CAC offers no allegations that either the Intermediary Cookie or DoubleClick ID Cookie (or any other cookie) was ever placed on any of the named Plaintiffs' browsers, or how. Plaintiffs' failure to allege facts showing they have "personally" been harmed precludes Article III jurisdiction. *Warth*, 422 U.S. at 502. The same outcome applies to Plaintiffs' general allegations about the collection of

[8] In addition to failing to show any actual injury, Plaintiffs cannot show violation of any statute that would confer standing. Article III's standing requirement is not satisfied unless a plaintiff's allegations establish that the statute has actually been violated. *In re Google Inc. Privacy Policy Litig.*, No. 12-01382, 2012 WL 6738343, at *5-6 (N.D. Cal. Dec. 28, 2012) (deficient Wiretap Act claim is insufficient to confer Article III standing). As explained in Section II below, Plaintiffs' allegations show that the statutes they assert do not apply to the facts alleged in the CAC. Merely reciting statutory claims does not confer Article III standing.

"Personally Identifiable Information." *See* CAC ¶ 3. The factual allegations and documents incorporated by reference in the CAC show that Google obtained no personal information by placing the cookies on browsers. *See supra* pp. 9-11. The only item allegedly sent to Google because of the placement of cookies is the value of the cookie itself—a simple string of text. *See id.*; CAC ¶¶ 46, 78. Thus, even if Plaintiffs had alleged an injury based on the supposed "collection" of personal information, that injury would not be "fairly traceable to the challenged action of [Google]," as required for Article III standing.

B. The Alleged Collection of "Personal Information" Does Not Confer Standing

Even if personal information had been gathered by cookies Google placed, courts have repeatedly held that there is no Article III injury where a plaintiff makes nothing more than general allegations that the value of his or her "personal information" was diminished by its collection and use. *See, e.g.*, *In re Google Inc. Privacy Policy Litig.*, No. 12-01382, 2012 WL 6738343, at *5 (N.D. Cal. Dec. 28, 2012) (the law does not confer "standing on a party that has brought statutory or common law claims based on nothing more than the unauthorized disclosure of personal information, let alone an unauthorized disclosure by a defendant to itself"); *Low v. LinkedIn Corp.*, No. 11-01468, 2011 WL 5509848, at *3-4 (N.D. Cal. Nov. 11, 2011) (dismissing for lack of standing claims that relied on general allegations that consumer information is valuable but failed to explain how collection of such information foreclosed plaintiff from capitalizing on any such value); *LaCourt v. Specific Media, Inc.*, No. 10-1256, 2011 WL 1661532, at *5 (C.D. Cal. Apr. 28, 2011) ("Plaintiffs do not explain how they were 'deprived' of the economic value of their personal information simply because their unspecified personal information was purportedly collected by a third party"); *Del Vecchio v. Amazon.com Inc.*, No. 11-366, 2011 WL 6325910, at *3 (W.D. Wash. Dec. 1, 2011) ("*Del Vecchio I*") ("While it may be theoretically possible that Plaintiffs' information could lose value as a result of its collection and use by Defendant, Plaintiffs do not plead any facts from which the Court can reasonably infer that such devaluation occurred in this case."); *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d

299, 327 (E.D.N.Y. 2005) (rejecting argument "that an individual [airline] passenger's personal information has or had any compensable value in the economy at large").

LaCourt and *Del Vecchio I* are directly on point as both cases involve allegations about a defendant's use of cookies. In *LaCourt*, the plaintiffs accused an online third-party advertising network of installing cookies on their computers to circumvent user privacy controls and to track Internet use without user consent. 2011 WL 1661532, at *7-13. The court held that the plaintiffs lacked Article III standing because (1) they had not alleged that any named plaintiff was actually harmed by the defendant's alleged conduct and (2) they had not alleged any "particularized example" of injury, but instead offered only abstract concepts, such as "opportunity costs," "value-for-value exchanges," "consumer choice," and "diminished performance." *Id.*

Similarly, in *Del Vecchio I*, the plaintiffs accused Amazon.com of placing tracking cookies on their browsers "against their wishes by 'exploiting' a known frailty in the cookie-filtering function" of the browsers in order to collect the plaintiffs' browsing history and other allegedly personal information. 2011 WL 6325910, at *1. The plaintiffs alleged that Amazon.com's use of cookies to obtain their information caused them "'economic harms,' including 'lack of proper value-for-value exchanges, undisclosed opportunity costs, devaluation of personal information, [and] loss of the economic value of the information as an asset.'" *Id.* Despite these allegations, the court dismissed the complaint, concluding that "Plaintiffs have simply not plead adequate facts to establish any plausible harm." *Id.* at *7.

Here, Plaintiffs' vague and conclusory allegations that they "gave up more personal information in their dealings with Google than they would have," "received less privacy from Google than promised them," and "lost the opportunity to sell the personal information at full value," CAC ¶¶ 242-244, are equally deficient and cannot confer Article III standing. Plaintiffs make the same allegations about diminished value of their personal information that were rejected by the *LaCourt* and *Del Vecchio I* courts as implausible and lacking any "particularized example." Plaintiffs allege no facts to show that anyone was willing to pay them specifically for their limited, individual browsing history allegedly obtained by Google. Nor do Plaintiffs allege

any facts showing that they attempted to sell that information and were unable to do so because of Google's alleged actions. While Plaintiffs make several allegations about the purported quantifiable value of *other* types of information related to online activities, *see id.* ¶¶ 56-67, none of these allegations identifies a lost opportunity by Plaintiffs to sell their history of visiting websites that display Google ads—and that is the information at issue here. Plaintiffs' allegations about their personal information thus do not establish an actual and concrete injury.

This action should therefore be dismissed under Rule 12(b)(1) for lack of Article III standing and thus, lack of subject matter jurisdiction.

III. THIS ACTION SHOULD BE DISMISSED UNDER RULE 12(B)(6) FOR FAILURE AND INABILITY TO STATE A CLAIM

A. Legal Standard

Under Rule 12(b)(6), a complaint should be dismissed when it "fail[s] to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). "[O]nly a complaint that states a plausible claim for relief survives a motion to dismiss." *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009) (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556 (2007)). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.* at 678. Similarly, the court must "disregard 'naked assertions devoid of further factual enhancement.'" *Santiago v. Warminster Twp.*, 629 F.3d 121, 131 (3d Cir. 2010) (quoting *Iqbal*, 556 U.S. at 678). Accordingly, while the Court accepts as true all material allegations in the complaint, it need not accept the truth of conclusory allegations or unwarranted inferences, nor should it accept legal conclusions as true merely because they are cast in the form of factual allegations. *Iqbal*, 556 U.S. at 678-79; *Santiago*, 629 F.3d at 131-133.

The CAC should be dismissed because Plaintiffs fail to allege essential elements for each cause of action that they assert. In most instances Plaintiffs allege nothing more than "threadbare recitals of the elements of a cause of action" or "naked assertions devoid of further factual enhancement."

B. The Federal Wiretap Claim (Count I) Should be Dismissed

The purpose of the federal Wiretap Act is to protect the contents of communications from intentional interception by persons who are not parties to the communication. *Bartnicki v. Vopper*, 532 U.S. 514, 523 (2001); *United States v. Reed*, 575 F.3d 900, 916 (9th Cir. 2009). The communications at issue in this case are those between Plaintiffs' browsers and Google. CAC ¶¶ 41, 205. Plaintiffs' wiretap claim should be dismissed because (1) Google was a party to the allegedly intercepted communications or had the prior consent of a party to the communication and (2) Plaintiffs cannot show that Google intercepted the content of any "communication" covered by the Wiretap Act.

1. Google Was Either a Party to the Alleged Communications or Had the Prior Consent of a Party to the Communication

It is not unlawful under the Wiretap Act for someone who is a "party to the communication" or who had prior consent to receive the communication from one of the parties to the communication to intercept those communications.[9] 18 U.S.C. § 2511(2)(d); *see, e.g., In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 713 (N.D. Cal. 2011) (no wiretap violation where plaintiff's mouse click was a communication to defendant or to a third party requesting delivery to defendant).

Google was a party to the communications here. Google was a party to the exchanges of information that took place directly between it and Plaintiffs' browsers each time Plaintiffs' browsers viewed a website displaying Google ads. CAC ¶¶ 41, 86-90, 203-207. Plaintiffs make clear that their browsers communicated directly with Google in the context of requesting an ad: "the server hosting the publisher's webpage also instructs the user's web browser to send a GET request to Google." *Id.* ¶ 86; *see also id.* ¶ 41 ("webpage will subsequently respond to the browser, instructing the browser to send a "GET" request to the third-party company charged with serving the advertisements"). As Plaintiffs explain, that "GET" request is a

[9] Although a party to a communication can be liable for intercepting a communication where their purpose was to commit "any criminal or tortious act," Plaintiffs have not alleged and could not allege such facts. 18 U.S.C. § 2511(2)(d); *Caro v. Weintraub*, 618 F.3d 94, 100 (2d Cir. 2010) (intent must be to commit a tort or crime beyond the violation of the Wiretap Act itself).

communication of Browser-Generated Information directly between Plaintiffs' browsers and Google—their browsers submit the necessary information for Google to display an ad. *Id.* ¶¶ 41, 46. It is not unlawful for Google to "intercept" a communication that Plaintiffs send directly to it. 18 U.S.C. § 2511(2)(d).

But even if Google were not a direct party to the communications between Plaintiffs' browsers and websites displaying Google ads, and instead had only obtained them from the websites directly, Plaintiffs could not state a Wiretap Act claim. The websites that Plaintiffs allegedly visit that display Google ads would also parties to the communications with Plaintiffs' browsers, and those websites have authorized Google's access to the communications. *See, e.g.*, CAC ¶ 41. This prior consent vitiates an interception claim. *See* 18 U.S.C. § 2511(2)(d); *DoubleClick*, 154 F. Supp. 2d at 510, 514 ("DoubleClick-affiliated Web sites are 'parties to the communication[s]' from [browsers] and have given sufficient consent to DoubleClick to intercept them."). It would be "implausible to infer" that websites displaying ads from the doubleclick.net domain "have not authorized DoubleClick's access" because "the very reason clients hire DoubleClick is to target advertisements" to their website visitors. *Id.* In any event therefore, 18 U.S.C. § 2511(2)(d)'s party exception causes Plaintiffs' Wiretap Act claim to fail.

2. Google Did Not Intercept Any Content Covered by the Wiretap Act

To state a claim under the Wiretap Act, Plaintiffs must also show that Google intercepted the "content" of their communications through the use of an electronic, mechanical, or other device at the time the communication is being transmitted. 18 U.S.C. § 2510(4) (defining "intercept"), § 2511(1); *Walsh v. Krantz*, 386 F. App'x 334, 338-339 (3d Cir. 2010) (quoting); *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113-114 (3d Cir. 2004). Plaintiffs cannot do so.

The Wiretap Act defines the "contents" of a communication as "information concerning the substance, purport, or meaning of" a communication, leaving unprotected other information about the communication. 18 U.S.C. § 2510(8); s*ee Reed*, 575 F.3d at 916; *Gilday v. Dubois*,

124 F.3d 277, 296 n.27 (1st Cir. 1997).[10] And courts routinely reject efforts to expand the Wiretap Act to cover mere transactional information about a communication or information about the parties to a communication because that is not "content." *See, e.g.*, *iPhone II*, 844 F. Supp. 2d at 1061-62 (data conveying the geolocation of plaintiff iPhone users was not covered by the Wiretap Act); *Sams v. Yahoo!, Inc.*, No. 10-5897, 2011 WL 1884633, at *6-7 (N.D. Cal. May 18, 2011) (Wiretap Act did not cover records identifying person using particular Yahoo ID and email address, IP addresses, and login times); *In re § 2703(d) Order*, 787 F. Supp. 2d 430, 435-36 (E.D. Va. 2011) (Act did not cover unique Internet Protocol ("IP") number, Twitter subscriber, user, and screen names, addresses, including e-mail addresses, telephone or instrument number or other subscriber number or identity, and temporarily assigned network address); *Gilday*, 124 F.3d at 296 n.27 ("the PIN of [a] caller, the number called, and the date, time and length of the call"); *Jessup-Morgan v. Am. Online, Inc.*, 20 F. Supp. 2d 1105, 1109 (E.D. Mich. 1998) (identity of user); *Reed*, 575 F.3d at 916 (data about telephone call, including time of origination, duration, source, and destination).

Plaintiffs cannot show that Google intercepted any information concerning the "substance, purport, or meaning"—*i.e.*, the "contents"—of any communication. *See* 18 U.S.C. § 2510(4), 2511(1). The *only* item at issue that would not have been communicated to Google but for the placement of a cookie is the cookie's value. *See* CAC ¶ 46; *supra* pp. 9-11. And the string of text that makes up a cookie value does not include the "contents" of any communication. It is merely a string of numbers and letters unrelated to the communications it accompanies (*e.g.*, id="225f401f5201002e||t=1328801360|et=730|cs=002213fd4890910dc3faab6200"). CAC ¶ 78. It conveys no information concerning the substance, purport, or meaning of any of Plaintiffs' communications. *See supra* pp. 4-5, 9. It is no more the "content" of a communication than the phone numbers, Internet Protocol addresses, and other trans-

[10] The Wiretap Act's purpose is to protect the substance of communications *intentionally communicated* from one person to another, "such as the words spoken in a phone call," and the Wiretap Act is "limited to information the user intended to communicate." *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012) ("*iPhone II*").

actional information that courts have held is excluded from protection. As such, it is beyond the scope of the Wiretap Act.[11]

3. Because There Was No Unlawful Interception, Plaintiffs Cannot State Use and Disclosure Claims

Plaintiffs make vague and conclusory allegations that Google "disclosed" and "used" unlawfully intercepted communications. *See* CAC ¶ 211. However, because Plaintiffs cannot show any unlawful interception, they cannot show an unlawful disclosure or use. 18 U.S.C. § 2511(1)(c)-(d) (creating liability only for use and disclosure of information "obtained in violation of this subsection"); *see also In re High Fructose Corn Syrup Antitrust Litig.*, 216 F.3d 621, 625 (7th Cir. 2000); *Meredith v. Gavin*, 446 F.2d 794, 799 (8th Cir. 1971); *Buckingham v. Gailor*, No. 00-1568, 2001 WL 34036325, at *6 (D. Md. Mar. 27, 2001), *aff'd*, 20 F. App'x 243 (4th Cir. 2001); *Betancourt v. Nippy, Inc.*, 137 F. Supp. 2d 27, 31-32 (D.P.R. 2001); *Simmons v. Sw. Bell Tel. Co.*, 452 F. Supp. 392, 396-97 (W.D. Okla. 1978), *aff'd*, 611 F.2d 342 (10th Cir. 1979). Where an interception is lawful, there can be no liability for use or disclosure of that communication.

C. The Stored Communications Act Claim (Count II) Should be Dismissed

The Stored Communications Act ("SCA") renders liable whoever "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication *while it is in electronic storage in such system*." 18 U.S.C. § 2701(a) (emphasis added).

[11] Plaintiffs' wiretap claim is also deficient because they cannot show that Google "intentionally" intercepted a communication. 18 U.S.C. § 2511(1). To show intent, Plaintiffs rely solely on the allegation that Google "has never provided any explanation," "any test data, analyses, studies or . . . theories" to show that the results caused by Safari's One In, All In Rule were "accidental." CAC ¶¶ 106-107. That allegation is inadequate because it alleges "facts that are 'merely consistent with' a defendant's liability" and "'stops short of the line between possibility and plausibility.'" *Iqbal*, 556 U.S. at 678.

1. Plaintiffs Cannot Identify a Communication in Electronic Storage

Plaintiffs' SCA claim fails because they cannot show that Google accessed anything that was in "electronic storage." Plaintiffs expressly allege that their communications were *not* in "storage" when Google accessed them. In their attempt to state a claim under the Wiretap Act, Plaintiffs go to great lengths to show that the communications Google allegedly obtained were "in transit" and accessed "contemporaneously with the transmission of those communications." *See* CAC ¶ 208. That allegation precludes Plaintiffs' SCA claim.

But Plaintiffs' SCA claim fails to satisfy the storage requirement for additional reasons, as well. Plaintiffs allege that cookies were placed on browsers on their computers or cell phones, but information "that an individual stores to his hard drive or cell phone is not in electronic storage under the statute." *Garcia v. City of Laredo, Tex.*, No. 11-41118, 2012 WL 6176479, at *3 (5th Cir. Dec. 12, 2012). "'Electronic storage' as defined encompasses only the information that has been stored by an electronic communication service provider" such as "information that an Internet provider stores to its servers or information stored with a telephone company – if such information is stored temporarily pending delivery or for purposes of backup protection." *Id.* (citing *Freedom Banc Mortg. Servs., Inc. v. O'Harra*, No. 11-01073, 2012 WL 3862209, at *8-9 (S.D. Ohio Sept. 5, 2012) ("'Electronic storage' as defined [by § 2510(17)] encompasses only the information that has been stored by an electronic communication service provider."); *see also DoubleClick*, 154 F. Supp. 2d at 511-12 ("[a]ny temporary, intermediate storage describes an e-mail message that is being held by a third party Internet service provider"); *iPhone II*, 844 F. Supp. 2d at 1058-59 (same).

Just like in *Garcia*, Plaintiffs here cannot show that the DoubleClick ID Cookie was accessed by Google while in "electronic storage" because information stored on Plaintiffs' personal devices is not "stored by an electronic communication service provider" in the provider's facility. Neither Plaintiffs, their devices, nor their browsers qualify as "electronic communication service providers." *DoubleClick*, 154 F. Supp. 2d at 511 ("Clearly, the cookies' residence

on plaintiffs' computers does not fall into § 2510(17)(B) because plaintiffs are not 'electronic communication service' providers").

2. Plaintiffs Cannot Identify a Facility Under the SCA

The lack of an SCA-covered "facility" is also fatal to Plaintiffs' SCA claim. A personal computer or mobile device is not a "facility through which an electronic communication service is provided." *Garcia*, 2012 WL 6176479, at *2-3 (citing cases). The "facilities" the SCA covers are Internet service providers (ISPs), telephone companies, and the like, not the computers used to access the electronic communication services those entities operate. *Id.* (citing *United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003) (the SCA does not cover information stored on a computer's hard drive); *Freedom Banc Mortg. Servs., Inc.*, 2012 WL 3862209, at *9 (computers are not protected "facilities" under the SCA); *iPhone II*, 844 F. Supp. 2d at 1057-58 (same for mobile devices)). Plaintiffs' theory that their computers or mobile devices are "facilities" through which their browsers provide "electronic communication services" (*see* CAC ¶¶ 216-18) is inconsistent with that term's meaning and usage in the Wiretap Act and has been consistently rejected by courts that have examined the issue, as recognized in *Garcia* and the other cases cited above.

3. Plaintiffs Cannot Show that Google's Access Was Unauthorized

Plaintiffs cannot show that Google's access to its own cookies was unauthorized, an essential element of an SCA claim. One court has already dismissed an SCA claim against Google's DoubleClick ad service, holding that DoubleClick was authorized to access its own cookies. *DoubleClick*, 154 F. Supp. 2d at 513-14 (citing 18 U.S.C. § 2701(c)(2)). Here, as in *DoubleClick*, Google was authorized to access its cookies. Having placed cookies in the normal course of interacting with browsers as they were designed by Apple and Microsoft to function, Google then "accessed" the cookies when they were sent back to Google among the Browser-Generated Information *Plaintiffs' browsers* submitted to Google so that it could deliver ads. Any access was thus fully authorized.

D. The Federal Computer Fraud Claim (Count III) Should be Dismissed

The Computer Fraud and Abuse Act (CFAA) was enacted to address "classic" computer "hacking," providing a civil cause of action for plaintiffs who have "suffer[ed] damage or loss" of $5,000 or more. *P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504, 510 (3d Cir. 2005); 18 U.S.C. § 1030(g). "Today, the CFAA remains primarily a criminal statute designed to combat hacking," and courts should not "contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to [defendants] who access computers or information in bad faith." *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 201, 207 (4th Cir. 2012); *accord United States v. Nosal*, 676 F.3d 854, 857-58 (9th Cir. 2012) (*en banc*) (refusing to "transform the CFAA from an anti-hacking statute into an expansive misappropriation statute" and construing CFAA to "maintain[] the CFAA's focus on hacking rather than turning it into a sweeping Internet-policing mandate"); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1130 (9th Cir. 2009) (CFAA "was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality"); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965-66 (D. Ariz. 2008) ("[T]he legislative history supports a narrow view of the CFAA. . . . The general purpose of the CFAA 'was to create a cause of action against computer hackers . . . Thus, the conduct prohibited is analogous to that of 'breaking and entering' . . . Simply stated, the CFAA is a criminal statute focused on criminal conduct. The civil component is an afterthought.").

Plaintiffs' CFAA claim should be rejected because they cannot show injury, let alone satisfy the $5,000 "damage" or "loss" prerequisite to maintain a CFAA claim. Moreover, the CFAA is simply inapplicable to these facts. The CFAA was never intended to criminalize the normal interaction between websites and browsers using designed features and protocols, like those Plaintiffs allege here. The CFAA was instead intended to punish destructive computer hacking, something Plaintiffs do not and could not plausibly allege here.

1. Plaintiffs Cannot Show the Required "Damage" or "Loss"

The CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). "Loss" means "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). Only "economic damages" qualify as "losses" under the CFAA. *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 935 (9th Cir. 2004). The unauthorized collection, use, or disclosure of "personal information" is not cognizable CFAA "loss." *iPhone II*, 844 F. Supp. 2d at 1068 (citing cases); *DoubleClick*, 154 F. Supp. 2d at 525-26 (same); *see also Del Vecchio v. Amazon.com, Inc.*, No. 11-366, 2012 WL 1997697, at *4 (W.D. Wash. June 1, 2012) ("*Del Vecchio II*") ("*It is not enough to allege only that the [Plaintiffs'] information has value to Defendant; the term 'loss' requires that Plaintiffs suffer a detriment – a detriment amounting to more than $5,000.*") (emphasis in original).

Plaintiffs' CFAA claim fails because they cannot show the required damage or loss. They do not even attempt to allege any "damage" at all. *See* CAC ¶¶ 225, 226. And while Plaintiffs nakedly state they have suffered a "loss," they fail to allege facts supporting their claimed loss. *See id.* The only "injury" identified in the entire CAC is no injury at all and certainly not a cognizable CFAA "loss"—that Plaintiffs "gave up more personal information in their dealings with Google than they would have," "received less privacy from Google than promised them," and "lost the opportunity to sell the personal information at full value." *See id.* ¶¶ 242-244. As in *iPhone II* and *Del Vecchio II*, even if Plaintiffs had facts to support such a speculative and conclusory allegation (they do not), the alleged diminished value of their personal information cannot support a CFAA claim.

2. Plaintiffs Cannot Allege a $5,000 Loss

Plaintiffs' CFAA claim is also deficient because they do not and cannot allege facts sufficient to show that Google's alleged conduct caused them at least $5,000 or more in "loss" over a

one year period. 18 U.S.C. § 1030(c)(4)(A)(i)(I); *Del Vecchio II*, 2012 WL 1997697, at *4. Courts routinely reject threadbare allegations of a $5,000 loss where plaintiffs merely "couch[] their allegations in generalities," as Plaintiffs have here. *Id.* at *5; *see also iPhone II*, 844 F. Supp. 2d at 1066-67; *Bose v. Interclick, Inc.*, No. 10-9183, 2011 WL 4343517, at *7 (S.D.N.Y. Aug. 17, 2011); *LaCourt*, 2011 WL 1661532, at *6; *Oil States Skagit Smatco, LLC v. Dupre*, No. 09-4508, 2010 WL 2605748, at *3 (E.D. La. June 21, 2010). Plaintiffs' CFAA claim thus fails because they allege no facts showing that they have suffered a $5,000 economic loss.[12] Nor could they, where they have suffered no injury. *See supra* pp. 12-15.

3. Plaintiffs Cannot Show a Violation of the CFAA

Because Plaintiffs' are unable to reach the CFAA's damages threshold, the Court need not reach the other elements of Plaintiffs' CFAA claim. But even if Plaintiffs could assert $5,000 in "damages" or "loss," they cannot show that Google violated any of the three CFAA provisions alleged by committing (a) a "transmission offense," (b) an "unauthorized access offense," and (c) an "exceeding authorized access offense." *See* CAC ¶¶ 224-226.

a. Plaintiffs Fail to State a Transmission Offense

A transmission offense requires a showing that the defendant "knowingly cause[d] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[d] damage without authorization, to a protected computer." 18 U.S.C. § 1030(a)(5)(A). Plaintiffs must allege both actual damage to their computers and that the defendant intended to cause damage to their computers. *Kalow & Springnut, LLP v. Commence Corp.*, No. 07-3442, 2008 WL 2557506, at *4 (D.N.J. June 23, 2008) (dismissing CFAA claim where plaintiff failed to allege "that [defendant] intended to cause *harm*, i.e. actual intent"); *Oracle Corp. v. SAP AG*, 734 F. Supp. 2d 956, 964 (N.D. Cal. 2010) ("plaintiffs must allege and prove that [the defendant] specifically 'intended' to 'cause damage'"); *Devon Energy Corp. v.*

[12] Even if Plaintiffs had suffered a cognizable "loss," they cannot aggregate losses across the putative class's millions of disparate devices running different software to reach the $5,000 threshold. *DoubleClick*, 154 F. Supp. 2d at 524-26; *Bose*, 2011 WL 4343517, at *6-7; *LaCourt*, 2011 WL 1661532, at *6 n.4.

Westacott, No. 09-1689, 2011 WL 1157334, at *9-10 (S.D. Tex. Mar. 24, 2011) (collecting cases). Here, Plaintiffs cannot state a transmission offense because they fail to even mention any CFAA "damage." Plaintiffs further fail to allege any facts showing that Google intended to cause "damage" to Plaintiffs' computers.

b. Plaintiffs Fail to State an Unauthorized-Access Offense

Plaintiffs cannot state an unauthorized-access offense because they cannot show that Google intentionally accessed their devices without authorization and caused damage or loss. An unauthorized-access offense requires a showing that the defendant "intentionally accesse[d] a protected computer without authorization, and as a result of such conduct, cause[d] damage and loss." 18 U.S.C. § 1030(a)(5)(C). A "person uses a computer 'without authorization'" only if "the person has not received permission to use the computer *for any purpose*" or if the owner "has rescinded permission to access the computer and the defendant uses the computer anyway." *Brekka*, 581 F.3d at 1135 (emphasis added). Because the CFAA is "a statute meant to target hackers" and not "a vehicle for imputing liability to [those] who access computers or information in bad faith," the "rule of lenity" requires that the term "without authorization" be read "literally and narrowly" to avoid "turn[ing] ordinary citizens into criminals."[13] *WEC*, 687 F.3d at 203, 207 (quoting *Nosal*, 676 F.3d at 856).

Plaintiffs' unauthorized-access offense claim fails because, as discussed above, they make no attempt to show any "damage" and they fail to show any "loss." *See supra* p. 23. But it also fails because Plaintiffs cannot show that Google accessed their computers "without authorization." Any access Google made to Plaintiffs' browsers was only in ways that those browsers

[13] To the extent there were any question about the meaning or application of "authorization" here, the term must be read to avoid liability. *United States v. Santos*, 553 U.S. 507, 514 (2008) (plurality op.) ("The rule of lenity requires ambiguous criminal laws to be interpreted in favor of the defendants subjected to them."). This "familiar principle" from the rule of lenity applies with full force in civil cases applying criminal statutes. *Skilling v. United States*, 130 S. Ct. 2896, 2932 (2010) (quoting *Cleveland v. United States*, 531 U.S. 12, 25 (2000)); *accord Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004) (applying rule of lenity in a civil context to a statute that "has both criminal and noncriminal applications"); *Brekka*, 581 F.3d 1134-35 (same); *DoubleClick*, 154 F. Supp. 2d at 513 (applying lenity in civil action brought under the Wiretap Act).

were designed to communicate by Apple and Microsoft, *i.e.*, in ways that were authorized by Plaintiffs' browsers. And Google's access was made only in the context of an authorized exchange of information with Plaintiffs' browsers as part of the browsers' request for Google to display an ad. *See* CAC ¶ 41; *see also supra* p. 3. Plaintiffs' browsers were designed to allow Google access to place cookies in connection with this exchange. *See supra* pp. 6-9. Thus, this sort of access is not "without authorization" under the appropriate literal and narrow construction of that statutory term. Indeed, interactions between software applications as they were designed to function cannot amount to hacking and fall well outside the purview of the CFAA. Nor can Plaintiffs show that Google "intended" to access their computers without authorization. Plaintiffs do not allege that Google altered the normal design or operation of their browsers, changed any settings on the browsers, or any other facts to show that Google believed it was engaging in unauthorized and illegal activity.

c. Plaintiffs Fail to State an Exceeding-Authorization Offense

Plaintiffs cannot state an exceeding-authorized-access offense because they cannot show that Google "intentionally accesse[d] a computer without authorization or exceed[ed] authorized access, and thereby obtain[ed] . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). As explained above, Plaintiffs cannot show that Google acted without authorization because Plaintiffs' browsers were designed to accept cookies in the manner in which Google is alleged to have interacted with them. *See also supra* pp. 6-9, 21. Plaintiffs are further unable to show that Google obtained any "information" from the browsers because the only item received by Google as a result of the alleged conduct was something Google already had and knew: the value of the cookie it had placed. *See supra* pp. 9-11.

E. The California Computer Crime Law Claim (Count VII) Should Be Dismissed

Plaintiffs' California Computer Crime Law ("CCL") claim fails for essentially the same reasons as their CFAA claim: "the necessary elements of Section 502 do not differ materially from the necessary elements of the CFAA." *Multiven, Inc. v. Cisco Sys., Inc.*, 725 F. Supp. 2d

887, 895 (N.D. Cal. 2010). The CCL prohibits "tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Pen. Code § 502(a). Only someone "who suffers damage or loss by reason of a violation" may bring a civil action under the law. *Id.* § 502(e).

As with their CFAA claim, Plaintiffs' failure to plead any cognizable "damage" or "loss" defeats their CCL claim. *See supra* p. 23; *Nexsales Corp. v. Salebuild, Inc*., No. 11-3915, 2012 WL 216260, at *3 (N.D. Cal. Jan. 24, 2012) (dismissing both CFAA and Section 502 claims for failure to plead damage or loss).

Each subsection of the CCL that Plaintiffs assert also requires a showing that Google acted "knowingly" and "without permission," which Plaintiffs cannot do. Cal. Pen. Code § 502(c)(1), (2), (6), (7), (8); *see In re iPhone Application Litig.*, No. 11-02250, 2011 WL 4403963, at *13 (N.D. Cal., Sept. 20, 2011) ("*iPhone I*"). Plaintiffs cannot meet the CCL's knowledge requirement for the same reason they do not meet the CFAA's intent requirement: Google communicated with Plaintiffs' browsers as those browsers were designed to communicate by Apple and Microsoft. Plaintiffs do not allege that Google altered the normal design of their browsers, changed any settings on the browsers, or any other facts to show that Google believed it was engaging in unauthorized and illegal activity. *See supra* pp. 25-26. And a claim based on access that is accidental or inadvertent fails the knowledge element of Section 502. *People v. Hawkins*, 121 Cal. Rptr. 2d 627, 634 (Cal. Ct. App. 2002). Because Google communicated with Plaintiffs' browsers only in ways that those browsers were designed to communicate, Google did so "with permission" from Plaintiffs' browsers.

In addition to failing to allege damage, loss, and knowledge, Plaintiffs do not allege the individual elements required for the various subsections of the CCL that they assert.

CCL subsection (c)(1). Plaintiffs' subsection (c)(1) claim fails because they cannot show that Google "alter[ed], damag[ed], delet[ed], destroy[ed], or otherwise us[ed] any data, computer, computer system, or computer network in order to . . . devise or execute any scheme or artifice to defraud, deceive, or extort." Cal. Pen. Code § 502(c)(1). Google merely communicated

with Plaintiffs' browsers in ways that those browsers were designed to communicate without causing any alteration, damage, deletion, or destruction. And Plaintiffs have alleged no facts showing they were defrauded, deceived, or subjected to extortion.

CCL subsection (c)(2). Plaintiffs cannot state a claim under subsection (c)(2), because they cannot show that Google "knowingly accesse[d] and without permission t[ook], copie[d], or ma[de] use of any data" on Plaintiffs' browsers. Cal. Pen. Code § 502(c)(2). The only data Google obtained due to placing cookies on browsers was data it had permission to access: the values of its own cookies. *See supra* pp. 21, 25-26.

CCL subsection (c)(6). The subsection (c)(6) claim fails because Plaintiffs cannot show that Google "provide[d] or assist[ed] in providing a means of accessing" Plaintiffs' browsers. Cal. Pen. Code § 502(c)(6). Though "providing" is undefined by the statute, by its plain language, this subsection requires that Google have given some other third party a means of access to Plaintiffs' computing devices. *See Craigslist, Inc. v. Naturemarket, Inc.*, 694 F. Supp. 2d 1039, 1057-58 (N.D. Cal. 2010). Plaintiffs make no such allegation here. *See* CAC ¶ 258.

CCL subsection (c)(7). Plaintiffs' subsection (c)(7) claim cannot survive because they cannot show that Google caused itself or any third party to "access" their browsers without permission. Cal. Pen. Code § 502(c)(7). "Section 502 defines 'access' in terms redolent of 'hacking' or breaking into a computer," which "is different from the ordinary, everyday use of a computer." *Chrisman v. City of Los Angeles*, 65 Cal. Rptr. 3d 701, 704-05 (Cal. Ct. App. 2007). As explained above, there was no "hacking or breaking into a computer" here. When Plaintiffs' browsers visited websites displaying Google ads, Google was authorized to communicate with the browsers based on their design and how they were set. *See supra* pp. 21, 25-26.

CCL subsection (c)(8). Plaintiffs cannot make out a subsection (c)(8) claim because they cannot show that Google "[k]nowingly introduce[d] any computer contaminant into any computer, computer system, or computer network." Cal. Pen. Code § 502(c)(8). The definition of "computer contaminant" is limited to computer instructions designed to "usurp the normal operation of the computer, computer system, or computer network." Cal. Pen. Code § 502(b)(10).

The string of text that comprises a cookie is nothing close to the "computer contaminant" the CCL envisions. And Plaintiffs make no factual allegations to the contrary. CAC ¶ 261. Plaintiffs admit that Google's alleged conduct is attributable to the IE and Safari browsers' functioning precisely as they were designed to, "rather than by a 'contaminant' introduced to Plaintiffs' computers by Defendant to 'usurp' the 'normal operations' of those computers." *See supra* pp. 6-9; *see also In re Facebook Privacy Litig.*, No. 10-02389, 2011 WL 6176208, at *4 & n.8 (N.D. Cal. Nov. 22, 2011) (section 502(c)(8) is "aimed at viruses or worms and other malware" and not alleged abuse of a "standard web browser function").

F. The California Wiretap Claim (Count VIII) Should be Dismissed

As with Plaintiffs' federal Wiretap Act claim, Plaintiffs cannot state a wiretap claim under the California Invasion of Privacy Act, Penal Code § 630, *et seq*. (the "CIPA") because they cannot show that Google "willfully and without the consent of all parties to the communication, or in any unauthorized manner," intercepted, used, or disclosed the "contents or meaning" of a "communication" that is "in transit."[14] Cal. Pen. Code § 631(a)); CAC ¶ 266. Just as with the federal wiretap claim, Plaintiffs cannot state a CIPA claim because (1) they acknowledge facts showing that Google was an authorized party to the communication or had prior consent from a party to the communication, (2) they fail to allege that the content (or anything regarding the content) of a protected communication was intercepted, and (3) they cannot allege that Google "willfully" intercepted a protected communication. *See supra* pp. 16-19.

And just as under the federal statute, interception of a communication is actionable under CIPA only if the information obtained is substantive. Cal. Pen. Code § 631(a) (covering only the "contents or meaning" of the communication). Non-content information merely identifying a party to the communication is not covered—and the cookies in this case do not even do that.

[14] Even if Plaintiffs could allege a CIPA claim, that claim would be preempted by the Federal Wiretap Act. *In re Google Inc. St. View Elec. Commc'ns Litig.*, 794 F. Supp. 2d 1067, 1084-85 (N.D. Cal. 2011); *LaCourt*, 2011 WL 1661532, at *7; *Bunnell v. Motion Picture Ass'n of Am.*, 567 F. Supp. 2d 1148, 1154-55 (C.D. Cal. 2007).

See, e.g., *People v. Suite*, 161 Cal. Rptr. 825, 828 (Cal. Ct. App. 1980) (obtaining telephone numbers of callers does not reveal content of communications).

G. The California Invasion of Privacy Claim and Intrusion Upon Seclusion Claims (Counts IV and V) Should be Dismissed

Plaintiffs assert "invasion of privacy" and "intrusion upon seclusion" claims under California constitutional and common law. *See* CAC ¶¶ 228–237. "Intrusion upon seclusion" is just one of the four types of invasion of privacy claims, together with public disclosure of private facts, false light, and appropriation of name or likeness. *See Hill v. Nat'l Collegiate Athletic Ass'n*, 865 P.2d 633, 647 (Cal. 1994). Because the latter three claims do not apply here, Plaintiffs' "invasion of privacy" claim is essentially duplicative of the "intrusion upon seclusion" claim. The two claims will fall together, as Plaintiff cannot show that Google (1) invaded a legally private matter (2) in a manner "highly offensive to a reasonable person" or "constituting a serious invasion of privacy."[15] *Folgelstrom v. Lamps Plus, Inc.*, 125 Cal. Rptr. 3d 260, 264-65 (Cal. Ct. App. 2011) (constitutional invasion of privacy claim and common law intrusion upon seclusion claim both failed because Plaintiff could not show alleged conduct was "highly offensive"). California law "set[s] a high bar for an invasion of privacy claim." *Low v. LinkedIn Corp.*, No. 11-01468, 2012 WL 2873847, at *9 (N.D. Cal. July 12, 2012).

Plaintiffs fail to allege that Google intruded into a private place, conversation, or matter because the communications between Plaintiffs' browsers and the websites they visited displaying Google ads were not "private" as to Google: Google was party to them and would have been without regard to the presence of any cookies. *See supra* pp. 16-17.14 In any event, Google obtained no "private" personal information by using cookies. Google only received the cookie values themselves, which were previously known to Google. *See supra* pp. 9-11, 17-19. Plaintiffs' allegations that Google received Browser-Generated Information or personal information due to the placement or presence of the cookies cannot support Plaintiffs' claims be-

[15] Even if Plaintiffs could state a common law privacy claim, the claim on these facts would be preempted by the federal Wiretap Act. *See supra* n.14 (citing cases explaining Wiretap Act's preemption of state law claims).

cause that information would have been received independent of the placement of the cookies. *See supra* pp. 9-11. Consequently, Plaintiffs fail to allege any "intrusion" or "invasion" into a "private" matter.

Plaintiffs' further allegation that Google used the DoubleClick ID Cookie to correlate browsing information fails to show a "serious invasion of privacy" that would be "highly offensive to a reasonable person." *See Low*, 2012 WL 2873847, at * 9 (disclosure of browsing history not highly offensive). Indeed, Plaintiffs admit that users readily consent to disclose "their valuable personal information" simply to use Google's search and other services. CAC ¶ 277. And Plaintiffs cannot show that the practice of showing tailored ads based on anonymous, correlated Browser-Generated Information is "highly offensive to a reasonable person" when that practice is concededly well-known and ubiquitous. *See* CAC ¶¶ 19-20, 24, 41, 63; *see also Pharmatrak*, 329 F.3d at 14 ("Cookies are widely used on the internet by reputable websites to promote convenience and customization."); *Chance v. Avenue A, Inc.*, 165 F. Supp. 2d 1153, 1156 (W.D. Wash. 2001) ("[m]any web sites use cookie technology"); *DoubleClick*, 154 F. Supp. 2d at 504 (service created 100 million profiles to serve tailored ads using cookies.).

H. The California CLRA Claim (Count IX) Should Be Dismissed

The California Consumer Legal Remedies Act (Cal. Civ. Code §§ 1750, *et seq.* ("CLRA")) claim should be dismissed because Plaintiffs cannot allege (1) any "good or service" covered by the CLRA; (2) any "damage"; (3) any "purchase or lease"; or (4) that they provided a CLRA notice 30 days before filing an action for damages.

First, Plaintiffs' CLRA claim fails because the alleged conduct of placing cookies on browsers is a software activity, and the CLRA does not cover software, only transactions involving "tangible chattels." *See, e.g., Sony Gaming Networks & Customer Data Sec. Breach Litig.*, No. 11-2258, 2012 WL 4849054, at *20-21 (S.D. Cal. Oct. 11, 2012) ("California law is clear that software is not a tangible good or service for the purposes of the CLRA."); *iPhone I*, 2011 WL 4403963, at *10 (dismissing CLRA claim involving iPhone applications because "[s]oftware is neither a 'good' nor a 'service' within the meaning of the CLRA"); *Ferrington v.*

McAfee, Inc., No. 10-01455, 2010 WL 3910169, at *14, *18-19 (N.D. Cal. Oct. 5, 2010) ("the CLRA does not cover transactions relating to the sale or lease of software"); *see also* Cal. Civ. Code § 1761 (defining "services" as "services furnished in connection with the sale or repair of goods," and defining "goods" as "tangible chattels").

Second, Plaintiffs' CLRA claim fails because they allege no damages in the form of a "tangible increased cost or burden" caused by the alleged conduct. *Meyer v. Sprint Spectrum L.P.*, 200 P.3d 295, 299, 301 (Cal. 2009); *see also* Cal. Civ. Code §§ 1770, 1780(a); *Bower v. AT&T Mobility, LLC*, 127 Cal. Rptr. 3d 569, 578 (Cal. Ct. App. 2011); *Wehlage v. EmpRes Healthcare, Inc.*, 791 F. Supp. 2d 774, 784-85 (N.D. Cal. May 25, 2011); *iPhone I*, 2011 WL 4403963 at *9-10.

Third, Plaintiffs' CLRA claim fails because they allege no "transaction" that resulted in or was intended to result in a "purchase or lease of goods or services." *See, e.g.*, *Sony Gaming*, 2012 WL 4849054, at *20-21 ("because Plaintiffs did not 'purchase or lease' a 'good or service' Plaintiffs' CLRA claim must fail"; "the transaction must result or be intended to result in the sale or lease of goods or services to a consumer"); *Facebook*, 791 F. Supp. 2d at 717 (CLRA claim dismissed where users not required to make a purchase to use Facebook).

Fourth, Plaintiffs' CLRA claim fails because they did not provide the required written notice of the alleged CLRA violation 30 days prior to filing an action for damages. Cal. Civ. Code. § 1782 (notice of CLRA violation must be given "[t]hirty days or more prior to the *commencement of an action for damages*") (emphasis added); *Von Grabe v. Sprint PCS*, 312 F. Supp. 2d 1285, 1303-04 (S.D. Cal. 2003) (dismissing CLRA claim with prejudice for failure to satisfy the 30-day notice requirement); *Davis v. Chase Bank U.S.A., N.A.*, 650 F. Supp. 2d 1073, 1089 (C.D. Cal. 2009) (same). Contrary to their allegation that plaintiff Lourdes Villegas provided the required 30-day CLRA notice, Plaintiffs admit that she only provided notice on the same day her lawsuit was filed. *See* CAC ¶ 283 (alleging notice was sent on February 23, 2012); *Villegas v. Google Inc., et al.*, No. 12-00915, Dkt. No. 1 (N.D. Cal. Feb. 23, 2012). That is deficient, and the CLRA claim should be dismissed: "failure to give notice before seek-

ing damages necessitates dismissal with prejudice, even if a plaintiff later gives notice and amends." *Waller v. Hewlett-Packard Co.*, No. 11-0454, 2011 WL 6325972, at *5-6 (S.D. Cal. Dec. 16, 2011) (dismissing CLRA claim with prejudice) (quoting *Cattie v. Wal-Mart Stores, Inc.*, 504 F. Supp. 2d 939, 950 (S.D. Cal. 2007)).

I. The California Unfair Competition Claim (Count VI) Should Be Dismissed

The California unfair competition law (Cal. Bus. & Prof. Code § 17200 ("UCL")) claim should be dismissed because (1) Plaintiffs have not suffered any loss of money or property; (2) Plaintiffs cannot show that any injury was caused by the alleged unlawful conduct; and (3) the unfair competition claim is based on alleged violations of law in Plaintiffs' other claims and is thus coterminous with those claims, each of which should be dismissed as explained above.

Plaintiffs lack standing to assert a UCL claim because they cannot "establish a loss or deprivation of money or property sufficient to qualify as injury in fact, i.e., economic injury." *Kwikset Corp. v. Superior Court*, 246 P.3d 877, 885 (Cal. 2011) (citing Cal. Bus. & Prof. Code § 17204). "[N]o one may recover damages under the UCL . . . a private person may recover restitution only of those profits that the defendant has unfairly obtained from such person or in which such person has an ownership interest." *Californians for Disability Rights v. Mervyn's, LLC*, 138 P.3d 207, 212 (Cal. 2006) (citing *Bank of the West v. Superior Court*, 833 P.2d 545 (1992); *Korea Supply Co. v. Lockheed Martin Corp.*, 63 P.3d 937 (2003)). "[U]ninjured private persons" are precluded "from suing for restitution on behalf of others." *Id.* (citing Cal. Bus. & Prof. Code § 17203).

The named plaintiffs have not even attempted to show that they "personally" suffered any loss of money or property. *Kwikset*, 246 P.3d at 886 ("plaintiff filing suit now must establish that he or she has personally suffered such harm"). Plaintiffs likewise do not allege any "loss or deprivation of money or property sufficient to qualify as injury in fact, i.e., economic injury." *See id.* at 885. Plaintiffs merely allege that they "gave up more personal information in their dealings with Google than they would have," "received less privacy from Google than promised them," and "lost the opportunity to sell the personal information at full value." CAC

¶¶ 242-244. While Plaintiffs' allegation that they "lost the opportunity to sell [their] information at full value" could suggest some speculative economic injury, this unsupported allegation is deficient because Plaintiffs fail to allege any actual facts to demonstrate its plausibility (*i.e.*, a sale, attempted sale, or even a market) as required by *Iqbal*, 556 U.S. at 678. *See Del Vecchio II*, 2012 WL 1997697, at *4.

In *Del Vecchio II*, the court rejected a nearly identical "lost opportunity" allegation as deficient because it was "untethered to any fact-based allegation of actual depreciation" of their personal information. *Id.* at *4 n.5. Specifically, the plaintiffs failed to "allege that they attempted to sell their 'private information'" and "were rebuffed because Defendant had already sold or publicized that information." *Id.* As in *Del Vecchio II*, Plaintiffs here do not allege any facts to show that Google's conduct prevented them from obtaining money that they would otherwise have obtained.

Courts have repeatedly held that the loss of privacy or personal information does not meet the standing requirements of the UCL. *See, e.g.*, *Sony Gaming*, 2012 WL 4849054, at *15 (loss of "property value in one's information, do[es] not suffice as injury under the UCL"); *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 811 (N.D. Cal. 2011) ("several courts have held that the unauthorized release of 'personal information' does not constitute a loss of money or property for purposes of establishing standing under the UCL"); *iPhone I*, 2011 WL 4403963, at *14 (same); *Ruiz v. Gap, Inc.*, No. 07-5739, 2009 WL 250481 at *4 (N.D. Cal. Feb. 3, 2009), *aff'd*, 380 F. App'x 689, 692 (9th Cir. 2010) (rejecting argument that "unauthorized release of personal information constitutes 'loss of property' as that phrase is understood in [California unfair competition law]"); *Thompson v. Home Depot, Inc.*, No. 07-1058, 2007 WL 2746603, at *3 (S.D. Cal. Sept. 18, 2007) (alleged use for marketing purposes of plaintiffs' personal information provided in connection with credit card transactions was insufficient under UCL).

Even if Plaintiffs had suffered an "economic injury," they cannot show that it was "caused by, the unfair business practice or false advertising that is the gravamen of the claim." *Kwikset*, 246 P.3d at 885 (citing Cal. Bus. & Prof. Code § 17204). Plaintiffs allege no facts to

show that the placement of cookies on their browsers prevented them from selling their information. Nor do Plaintiffs allege any facts showing that they received less monetary compensation for their information than they would have but for the placement or presence of cookies on their browsers.

Finally, Plaintiffs' UCL claim also fails because it is predicated on the other "unlawful acts" alleged in the complaint and should be dismissed along with them. *Holomaxx Techs. v. Microsoft Corp.*, 783 F. Supp. 2d 1097, 1108 (N.D. Cal. 2011); *DocMagic, Inc. v. Ellie Mae, Inc.*, 745 F. Supp. 2d 1119, 1147 (N.D. Cal. 2010); *see also nSight, Inc. v. PeopleSoft, Inc.*, 296 F. App'x 555, 561 (9th Cir. 2008) (UCL "'borrows' violations from other laws making them independently actionable as unfair competitive practices") (quoting *Korea Supply Co. v. Lockheed Martin Corp.*, 63 P.3d 937, 943 (Cal. 2003)).

This action should therefore be dismissed under Rule 12(b)(6) for failure to state a claim.

CONCLUSION

For the foregoing reasons, Google respectfully requests that the Consolidated Amended Complaint be dismissed.

Respectfully submitted,

Dated: January 22, 2013

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

By: /s/ Michael H. Rubin

Michael H. Rubin, CA State Bar No. 214636
Anthony J Weibell, CA State Bar No. 238850
C. Scott Andrews, CA State Bar No. 243690
Wilson Sonsini Goodrich & Rosati, P.C.
650 Page Mill Road
Palo Alto, CA 94304-1050
650-493-9300
Email: mrubin@wsgr.com; aweibell@wsgr.com; sandrews@wsgr.com

Attorneys for Defendant
GOOGLE INC.